IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF:
THE RESIDENCE LOCATED AT
20 PEACEFUL DRIVE
CORTLAND, NEW YORK 13045

3:05-MJ-201 (DEP)

Application and Affidavit for Search Warrant

I, James T. Lyons, Jr., being duly sworn do depose and state as follows:

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) for eight years. I am currently assigned to the Albany Field Division, Binghamton, New York Resident Agency. I have investigated matters involving the sexual exploitation of children via computers and the internet, specifically those addressing violations of Title 18, United States Code, Section 2252A, which criminalizes the possession, receipt, and transmission of child pornography. I have made arrests and conducted searches pertaining to these types of

investigations.

2. This application and affidavit are made in support of a request for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Section 2252A, which criminalizes, among other things, the possession, receipt, and shipment of child pornography and other related materials. The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachment A.

3. The location to be searched is known as the residence of David J. Falso located at 20 Peaceful Drive, Cortland, New York, and this affidavit is submitted in support of a warrant to search the entire premises, including the residential dwelling and any computer and computer media located therein where the instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Section 2252A, as specified further in Attachment A, might be found.

4. The premises known as 20 Peaceful Drive, Cortland, New York, is a single story residence, white in color with blue trim, with attached garage. The name Falso appears on a black colored mailbox located directly in front of the 20 Peaceful Drive residence.

5. The statements contained in this application and affidavit are based in part on information provided by Special Agents of the FBI and on my experience and background as an Agent with the FBI. Since this affidavit is being submitted for the

limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause to believe that evidence of violation of Title 18, United States Code, Section 2252A, is located at the above address.

APPLICABLE LAW

6. Title 18, United States Code, Section 2252A, entitled "Certain activities relating to material constituting or containing child pornography", provides, in part, that

(a) Any person who -

(1) knowingly mails, or transports, or ships in interstate or foreign commerce by any means, including by computer, any child pornography;

(2) knowingly receives or distributes -

(A) any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer;

(3) knowingly

(A) reproduces any child pornography for distribution through the mails, or in interstate or foreign commerce by any means, including computer; or

(B) advertises, promotes, presents, distributes, or

solicits through the mails, or in interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains -

(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or

(ii) a visual depiction of an actual minor engaging in sexually explicit conduct;...

(5)(B) knowingly possess any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer,...

shall be punished as provided in subsection (b).

7. Per 18 USC § 2256(1), the term "minor" means any person under the age of eighteen years.

8. Per 18 USC § 2256(8), the term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in

sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

9. Per 18 U.S.C. § 2256(2)

(A) Except as provided in subparagraph (B), "sexually explicit conduct" means actual or simulated -

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the genitals or pubic area of any person;

(B) For purposes of subsection 8(B) of this section, "sexually explicit conduct" means -

(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(ii) graphic or lascivious simulated:

(I) bestiality;

(II) masturbation; or

(III) sadistic or masochistic abuse; or

(iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

DEFINITIONS

10. "Child Erotica" are materials or items that are sexually arousing to pedophiles but that are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. Former FBI SSA Kenneth Lanning, whose qualifications are discussed later, defines child erotica as follows:

> Any material, relating to children, that is sexually arousing to a given individual . . . [s]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids."

See Burgess, Ann, Child Pornography and Sex Rings, Ch. 4 authored by Kenneth Lanning, at p. 83 (Lexington books 1984).

11. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

12. "IP address" or "Internet Protocol address" refers to a

unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address - and that same number is used by the user every time his computer accesses the Internet.

13. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

14. "Sexually Explicit Conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital,

or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

15. "URL" or "Uniform Resource Locator" refers to Internet addresses. Each file on the Internet has a unique address called a Uniform Resource Locator, more commonly known as URL.

16. "Visual Depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. (See 18 U.S.C. § 2256(5)).

SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

17. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computer and their components, or seize most or all computer items (computer hardware, software, and related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-ROMs, and DVD drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine

which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

18. Based upon your affiant's consultation with experts in computer searches, data retrieval from computers and related media, and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output

peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their comparability with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them as soon as possible.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software

that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes of receipt, distribution and possession of child pornography, in violation of law, and should all be seized.

19. I have been advised by computer forensic experts and other experts who have conducted computer searches that people commonly store information on their computers, without periodically cleaning out all of their computer files. I also know that even if files, including graphic image files, have been deleted, they will be sent to a recycling bin. These files can easily be restored if they are retained in the recycling bin. A user can delete the files in the recycling bin, but as described below, the date is still on the computer. Even if a computer file has been deleted, the actual data in the file is not erased; only the index or directory to the file is deleted. The file remains stored on the hard drive of the computer in "slack space." ("Slack space" refers to space on a computer's hard drive that his available for use by the computer. As time passes, and space on the hard drive is needed for other functions, slack space is randomly overwritten with other data.). There is technology which would enable a computer forensic expert to retrieve files from "slack space". There is also currently software that allows an individual to delete all of the files in

the computer's "slack space."

SEARCH METHODOLOGY TO BE EMPLOYED

20. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to

appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

21. As a result of my training, experience and conversations with experts in the field, I know that computers are utilized by individuals who exploit children (which includes collectors of child pornography) to: a) correspond with like-minded individuals via e-mail, chat, bulletin boards, newsgroups, instant messages, file transfers and other means; b) store identifying information concerning child victims, as well as identifying information about other individuals who share the same interests; c) locate, view, download, collect and organize images of child pornography found through the Internet. Computers also afford individuals a degree of anonymity.

22. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. These online storage accounts are often free but can involve a charge. Payment is almost always made via credit card, debit card, or

other similar payment service.

23. A subscriber assigned a free online storage account frequently can set up such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a subscriber of a free online storage service, the service provider frequently will have no records in that subscriber's name. Instead, the online service will only be able to identify files, including child pornography, that are associated with a "login," or unique, user-created identity the subscriber uses to "log on" to the online service.

24. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the online service. Consequently, the illegal files have minimal contact with the subscriber's home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet.

25. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived or other files on the user's home computer. Other evidence can also be found through unique software that may exist on a user's home computer that has

been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of such accounts, but the login and password.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmark" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. In other words, if a computer user were to go to the website called "DOJ.gov", a "footprint" in the browser cache may be found pointing to that website, indicating that particular computer was used to visit that website.

YAHOO! Inc.

27. Yahoo! Inc. is a commercial computer service company that provides services to Internet users that include e-mail, Groups, Internet search capability, games, personal ads, chat, instant messaging, and other services. Many of the services offered by Yahoo are free to the user. Users of certain Yahoo services are required to register with Yahoo to obtain a Yahoo

ID.

a. A Yahoo ID is a unique identifier of a user's account. The registration process requires the selection of an ID (sometimes referred to as a screen name, Login Name, or profile), a password, and the voluntary supply of some personal information. This process is completed on line.

Example: Using Yahoo's Internet search engine does not require a Yahoo ID. However, using the Yahoo Games service or using the web features of the Yahoo Groups service does require a user to sign in using a Yahoo ID.

b. Up to six profiles can be associated with a single Yahoo ID. These Profiles are also known as aliases and allow the user to appear as someone other than their Yahoo ID when using certain Yahoo services. Other users of the service may be able to view profile information. Yahoo ID registration and profile information is supplied by the user and is not verified by Yahoo. Profile information can be listed or unlisted, similar to telephone listings.

FACTUAL BACKGROUND

28. On or about 07/31/2003, FBI Special Agent Todd Gentry, Kansas City Division, obtained the IP address of a website which advertised and contained child pornography. When the IP address, 207.36.140.60, was accessed via the Internet, a web page belonging to the CP Freedom Group was displayed. CyberGate Incorporated, of Fort Lauderdale, Florida, was the network administrator for this IP address. The website was hosted by

www.valueweb.net and contained approximately eleven images of child pornography. The website advertised additional child pornography, but the URL was hidden until a membership was purchased.

29. On or about 07/31/2003, FBI Special Agent Michael Daniels, Kansas City Division, acting in an undercover capacity, signed up for a one month membership. Special Agent Daniels was charged $99.00 for the membership and the $99.00 membership charge appeared to have been processed though Wells Fargo Bank. Special Agent Daniels subsequently received an e-mail from CP Freedom Group, registration@cp-freedom.com. The e-mail contained the URL www.cp-members.com, login: 300523, and password: 06587620. The e-mail stated that the membership was good for one month.

30. The website www.cp-members.com, IP address 216.180.251.147, was registered to CP Freedom Group which had a mailing address in San Francisco, California. The IP address was hosted by Net Depot, Inc. of Atlanta, Georgia. The domain name (www.cp-members.com) was registered through InterCosmos Media Group, Inc., of New Orleans, Louisiana, and the registrant was listed as Ded Moroz. A remote IP address of 66.118.166.80 was also listed on the InterCosmos account associated with Ded Moroz. The remote IP address was administered by Sago Networks, of Tampa, Florida.

31. In or about July 2004, Special Agent Todd Gentry reviewed the completed forensic examination of the website

hosting www.cpfreedom.com. The forensic examination revealed several hundred possible subscribers along with e-mail addresses and other information. In or about July 2004, subpoenas were served on appropriate ISP's for each e-mail address identified on the www.cpfreedom.com website. In or about September 2004, all subpoena requests were returned to the FBI. Pursuant to a review of the subpoenaed records, the following subscriber information (among others) was associated with the www.cpfreedom.com website: David J. Falso, 20 Peaceful Drive, Cortland, New York, Yahoo User ID: cousy1731@yahoo.com. Based upon investigation and examination conducted by Special Agent Todd Gentry and others, it appears that a person with the e-mail address of cousy1731@yahoo.com either gained access or attempted to gain access to the website www.cpfreedom.com. Special Agent Gentry's investigation and review of forensic examination revealed that the material associated with the www.cpfreedom.com website is hardcore child pornography.

32. In or about December 2004, your affiant obtained a New York State Police report regarding David J. Falso, of 20 Peaceful Drive, Cortland, New York. A review of this report revealed that on or about 02/18/1987, Falso was arrested by the New York State Police and Falso was charged with Sexual Abuse and Endangering the Welfare of a Child. The report reflected that Falso sexually abused a seven year old female when he placed his hands inside the female's underwear and digitally penetrated the female. The female informed the New York State Police that she referred to

Falso as "Cousey". Falso was interviewed by a New York State Police Investigator and Falso admitted he tickled the female and may have gone too far. Falso also admitted to the New York State Police Investigator that he (Falso) may have latent problems and that he might require some type of counseling. On or about 09/21/1987, Falso pleaded guilty to Acting in a Manner Injurious to a Child less than Sixteen, a New York State Class A Misdemeanor, for which Falso received a sentence of three years probation.

33. On or about 04/04/2005, pursuant to a subpoena issued to New York State Electric and Gas (NYSEG), NYSEG provided records which reflect that Falso has a current utilities account at 20 Peaceful Drive, Cortland, New York. The records further reflect that on or about 10/15/1984, Falso initially established the NYSEG utilities account at 20 Peaceful Drive, Cortland, New York.

34. On or about 04/12/2005, pursuant to a subpoena issued to Yahoo! Inc., Yahoo provided records which reflect that Falso has an active Yahoo account. Falso has a Yahoo login name of "cousy1731" and a Yahoo e-mail address of cousy1731@yahoo.com. Falso's Yahoo account was established on or about 06/02/1998 and the residential address associated with Falso's Yahoo account is listed as 20 Peaceful Drive, Cortland, New York, 13045. The Yahoo records also reflect that Falso's Yahoo account was accessed on a regular basis during the period 03/21/2005 - 04/10/2005. Additionally, the Yahoo records reflect that Falso

has an alternate e-mail address of dfalso1@twcny.rr.com.

35. On or about 05/20/2005, pursuant to a subpoena issued to Time Warner Cable, Time Warner Cable provided records which confirmed that Falso has an active Time Warner Cable Road Runner account of "dfalso1". The records also reflect that Road Runner service was established at Falso's residence, 20 Peaceful Drive, Cortland, New York, on or about 02/09/2004. As of 05/20/2005, Falso's Road Runner account was still active. Based upon the fact that Falso has active Road Runner service at 20 Peaceful Drive, Cortland, New York, it is logical to infer that Falso possesses a computer at 20 Peaceful Drive, Cortland, New York, to access the aforementioned Road Runner service.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

36. I have discussed the facts of this investigation with Special Agent David C. Fallon, the Crimes Against Children/Innocent Images National Initiative Coordinator for the FBI Albany Division. Special Agent Fallon has consulted with FBI Supervisory Special Agent (SSA) James T. Clemente who has worked in the Behavioral Analysis Unit of the FBI since 1998. SSA Clemente has been a Special Agent with the FBI since 1987. As a member of the Behavioral Analysis Unit, SSA Clemente consults on child exploitation cases throughout the United States, South America, and certain European and African countries. Since 1998, he has received three Exceptional Performance Awards from the Department of Justice and a Superior Service Award from the FBI. In addition, he has received numerous letters of commendation

from state, federal, and local law enforcement in connection with his work in the Behavioral Analysis Unit.

37. SSA Clemente's training has involved a significant number of specialized courses in the area of child exploitation, including, but not limited to the following: Innocent Images On-Line Sex Crimes Against Children; National Crimes Against Children; On-Line Sex Crimes Against Children; Clinical Forensic Psychology; Behavioral Analysis of Violent Crime; Missing and Exploited Children Seminar; Research Methodologies; MO, Ritual & Signature Advanced Seminar; and Criminology. In addition, he has mentored under, worked with, studied the articles of, and taught with Kenneth V. Lanning, a Supervisory Special Agent, FBI (retired as of October, 2000). SSA Lanning has, over the past 27 years, authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work forms the basis of the behavioral analysis performed by the FBI in child exploitation cases.

38. SSA Clemente has assisted in the writing of numerous search warrant affidavits and has testified as an expert witness in federal court in the areas of child sex offender behavior, child sexual victimology and child pornography. He has given over 100 presentations and lectures to local, state and federal law enforcement agencies, prosecutors, and health care professionals throughout the United States on various topics related to child exploitation, including, but not limited to the following topics: Behavioral Analysis of Child Sex Crimes

Offenders, On-Line Sex Crimes Against Children, and Equivocal Death Investigations.

39. As a member of the Behavioral Analysis Unit, SSA Clemente has analyzed and consulted on between one and two hundred child sexual exploitation and victimization cases a year. His analyses are based on all available evidence, including chat records, image collection analysis, collection themes, possession of erotica, possession of sexual paraphernalia, fantasy literature and writings, other relevant acts, and background information. The vast majority of the cases he has analyzed have involved either Preferential or Situational Sex Offenders. His role in these cases has varied as follows: from analyzing investigative results for the purpose of making investigative suggestions, to providing expert affidavits for search warrant applications, to providing interview strategies for subjects and victims, to consulting with local, state and federal prosecutors on trial strategies. In addition, SSA Clemente has interviewed between 80 and 100 offenders himself. A behavioral assessment is not a clinical diagnosis, rather it is a law enforcement tool used to identify and predict offender behavior.

40. SSA Clemente has advised Special Agent Fallon of the following traits and characteristics that are generally found to exist and be true in cases involving individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children.

They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

d. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each

other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

e. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

f. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

41. The following court decisions support some of these conclusions:

A. United States v. Ricciardelli, 998 F.2d 8, 12, n. 4 (1st Cir. 1993). ("[H]istory teaches that collectors [of child pornography] prefer not to dispose of their dross, typically

retaining obscene materials for years.");

B. United States v. Winningham, 953 F.Supp. 1068, 1079, n. 19 (D.Minn. 1996). (Formalized opinion concerning proclivities of pedophiles are not always necessary in a search warrant affidavit, since there is a "commonsensical inference that those who treasure such prurience do so for extended viewing, and for trafficking with others who share the same persuasion.");

C. United States v. Lamb, 945 F.Supp. 441, 460(N.D.N.Y. 1996)("The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal courts: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.").

42. Based upon my training and experience, conversations with Special Agent Fallon, case law, information provided by SSA Clemente as well as SA's Todd Gentry and Michael Daniels, and the facts listed in this affidavit, it is my opinion that there is

probable cause to believe that the individual utilizing the Yahoo ID "cousy1731" and the Road Runner ID "dfalso1" is a collector of child pornography.

CONCLUSION

43. Based upon all of the information set forth in this application, including information provided by SSA Clemente, SA David Fallon, SA Todd Gentry, and SA Michael Daniels, your affiant respectfully submits that there is probable cause to believe that the individual utilizing the Yahoo ID "cousy1731" and Road Runner ID "dfalso1", using a computer located at 20 Peaceful Drive, Cortland, New York, the residence of David J. Falso, violated Title 18, U.S.C., Sections 2252 and 2252A by receiving and possessing child pornography and that evidence of this crime, listed in Attachment A and made part of this application and affidavit, is probably located at said address.

JAMES T. LYONS, JR.
Special Agent, FBI

SUBSCRIBED TO AND SWORN TO
BEFORE ME THIS 1st th DAY
OF JUNE, 2005

THOMAS J. MCAVOY
SENIOR JUDGE, UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search the premises known as 20 Peaceful Drive, Cortland, New York, which is more specifically identified in the body of the application, including any computers, associated storage devices and/or other devices located therein that can be used to store information and/or connect to the Internet, for records and materials evidencing a violation of Title 18, United States Code, Sections 2252 and 2252A, which criminalizes, in part, the possession, receipt and transmission of child pornography (defined in 18 U.S.C. § 2256), as more specifically identified below:

1. Any and all tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive, terminals (keyboards and display screens) and other computer related operation equipment, in addition to computer photographs, digital graphic file formats and/or photographs, slides or other visual depictions of such digital graphic file format equipment that may be, or are used to visually depict child pornography, child erotica, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession, or receipt of child pornography, child erotica or information pertaining to an interest in child

pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.

4. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, including , but not limited to, evidence of the e-mails sent to and/or from "cousy1731" and "dfalso1".

5. In any format and media, all originals, copies and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or child erotica.

6. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages) identifying persons transmitting through interstate or foreign commerce, including via computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code,

Section 2256, or child erotica.

7. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital data files and web cache information), bearing on the receipt, shipment or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

8. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.

9. Evidence of association, by use, subscription or free membership, with online clubs, groups, services or other Internet sites that provide or otherwise make accessible child pornography.

10. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.

11. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

12. Records, in any format or media, evidencing ownership or use of computer equipment and paraphernalia found in the residence to be searched, including, but not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, handwritten notes and handwritten notes in computer manuals.